Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
06/06/2019	1.0	M. Elbanhawi	First submissio

Table of Contents

Purpose of the Technical Safety Concept

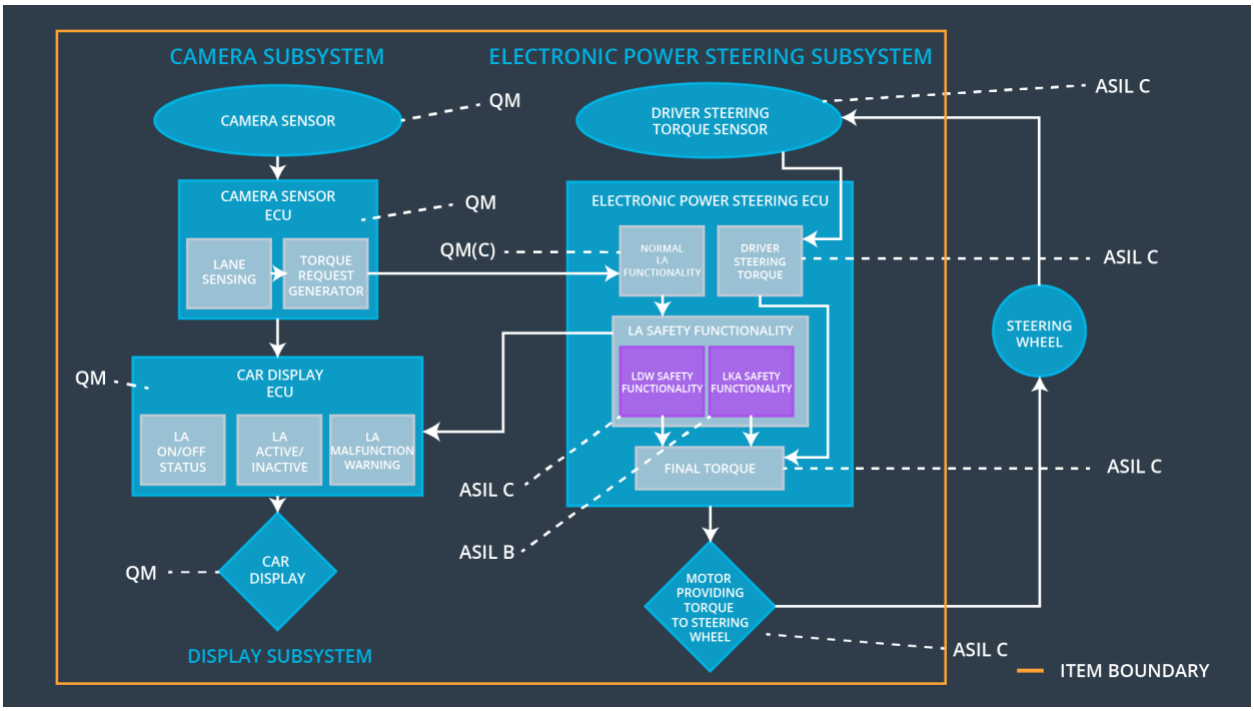
The purpose of the technical safety concept is to derive technical requirements from functional safety requirements, assign them an ASIL and a component. Technical requirements inherent ASIL from functional safety requirements. Technical requirements are more detailed than functional safety requirements, hence, they are assigned to components in the architecture.

Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Set the oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Set the oscillating torque amplitude to 0
Functional Safety Requirement 02-01	The electronic power steering ECU shall limit lane keeping assistance torque for only Max_Duration	B	500 ms	Set the oscillating torque amplitude to 0

Refined System Architecture from Functional Safety Concept

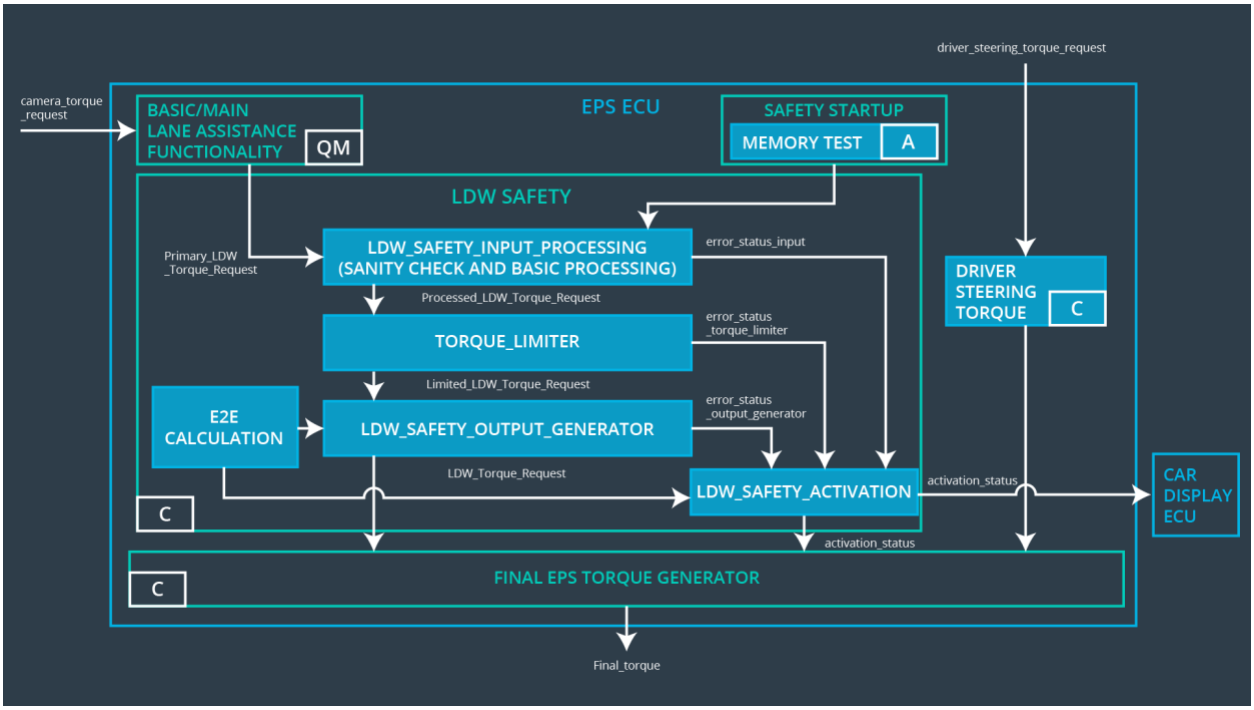


Functional overview of architecture elements

Element	Description
Camera Sensor	Capture images of the road and send to the camera ECU
Camera Sensor ECU - Lane Sensing	Software module that processes images to determine lane and position of vehicle in lane
Camera Sensor ECU - Torque request generator	Software module the sends a torque request based on the lane sensing output to the power steering ECU
Car Display	HMI to the driver, displays light status for LKA and LDW
Car Display ECU - Lane Assistance On/Off Status	Indicates the status of Lane Assistance
Car Display ECU - Lane Assistant Active/Inactive	Indicates the activity of Lane Assistance

Car Display ECU - Lane Assistance malfunction warning	Indicates the functionality of Lane Assistance
Driver Steering Torque Sensor	Measures the steering input from the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software block that receives torque input from the driver
EPS ECU - Normal Lane Assistance Functionality	Software block that receives torque request from Camera Sensor ECU – Torque request block
EPS ECU - Lane Departure Warning Safety Functionality	Software block that constrains the torque amplitude and frequency to Max_Torque_Amplitude and Max_Torque_Frequency respectively.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software block that limits the LKA activity duration to Max_Duration
EPS ECU - Final Torque	Software block that combines torque request from LKA, LDW and send it to the motor
Motor	Applies torque request to the steering wheel

Technical Safety Concept



Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Torque_Amplitude	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50ms	LDW Safety	Disable LDW

Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Disable LDW

Functional Safety Requirement 01-2 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below	C	50ms	LDW Safety	Disable LDW

	Max_Torque_Frequency				
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety	Disable LDW
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Disable LDW

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

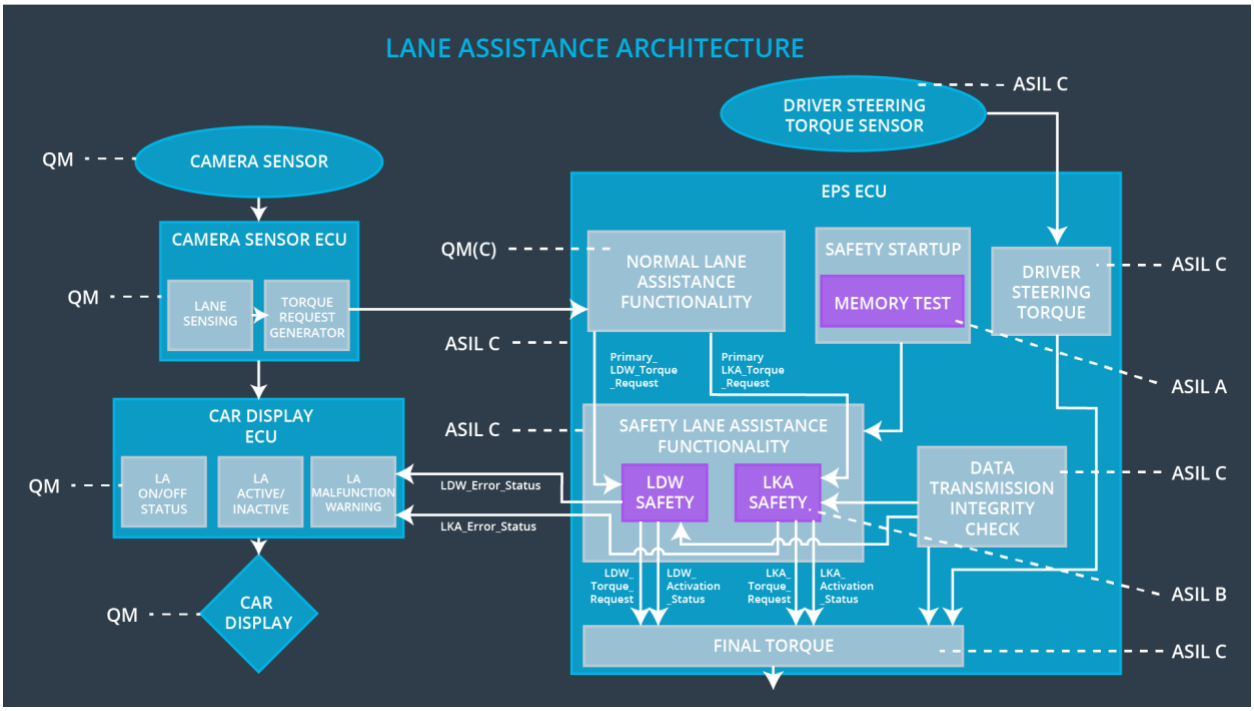
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional	The lane keeping item shall	X		

Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the LKA_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Duration	B	50ms	LKA Safety	Disable LKA
Technical Safety Requirement 02	The validity and integrity of the data transmission for LKA_Torque_Request Request signal shall be ensured	B	50ms	LKA Safety	Disable LKA
Technical Safety Requirement 03	As soon as a failure is detected by theLKA function, it shall deactivate the LKA feature and the LKA_Torque_Request shall be set to zero	B	50ms	LKA Safety	Disable LKA
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the LKA_Torque_Request block shall send a signal to the car display ECU to turn on a warning light	B	50ms	LKA Safety	Disable LKA
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Disable LKA

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Torque_Amplitude	**X**		
Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	**X**		

Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	**X**		
Technical Safety Requirement 01-01-04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	**X**		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	**X**		
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Torque_Frequency	**X**		
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	**X**		
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	**X**		
Technical Safety Requirement 01-02-04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	**X**		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	**X**		

Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the LKA_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Duration	**X**		
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for LKA_Torque_Request Request signal shall be ensured	**X**		
Technical Safety Requirement 02-01-03	As soon as a failure is detected by theLKA function, it shall deactivate the LKA feature and the LKA_Torque_Request shall be set to zero	**X**		
Technical Safety Requirement 02-01-04	As soon as the LKA function deactivates the LKA feature, the LKA_Torque_Request block shall send a signal to the car display ECU to turn on a warning light	**X**		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disable LDW	Malfunction_01, Malfunction_02,	Yes	LDW Malfunction Warning on Car Display
WDC-02	Disable LKW	Malfunction_03,	Yes	LKA Malfunction Warning on Car Display